

# Distribuisci interfaccia dati ridondante in Azure FTD Gestito da CD-FMC

## Sommario

---

---

## Introduzione

In questo documento viene descritto come configurare un FTD virtuale gestito da cdFMC in modo che utilizzi la funzionalità dell'interfaccia dati di accesso per manager ridondante.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Management Center
- Cisco Defense Orchestrator

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Centro gestione firewall distribuito tramite cloud
- Virtual Secure Firewall Threat Defense versione 7.3.1 ospitato in Azure Cloud.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Qualsiasi dispositivo fisico in grado di eseguire Firepower Threat Defense versione 7.3.0 o successive.

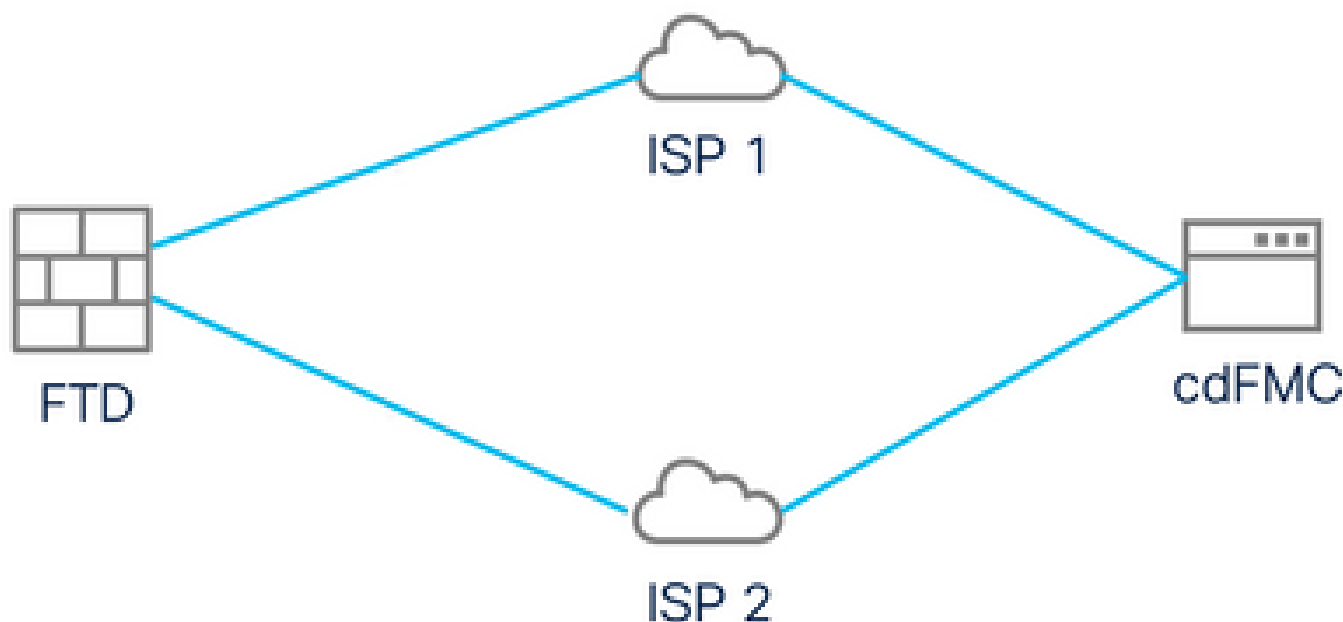
## Premesse

In questo documento viene illustrato come configurare e verificare un vFTD gestito da cdFMC per utilizzare due interfacce dati a scopo di gestione. Questa funzione è spesso utile quando i clienti hanno bisogno di una seconda interfaccia dati per gestire il loro FTD su Internet, utilizzando un secondo ISP. Per impostazione predefinita, l'FTD esegue un bilanciamento del carico a andata e ritorno per il traffico di gestione tra entrambe le interfacce. Tale bilanciamento può essere modificato in un'implementazione di Active/Backup come descritto in questo documento.

L'interfaccia dati ridondante per la funzionalità di gestione è stata introdotta in Secure Firewall Threat Defense versione 7.3.0. Si presume che il vFTD sia raggiungibile da un server dei nomi in grado di risolvere gli URL per l'accesso CDO.

## Configurazione

### Esempio di rete



Esempio di rete

### Configurazione di un'interfaccia dati per l'accesso alla gestione

Accedere al dispositivo tramite la console e configurare una delle interfacce dati per l'accesso alla gestione con il comando `configure network management-data-interface`:

```
<#root>
```

```
>
```

```
configure network management-data-interface
```

*Note: The Management default route will be changed to route through the data interfaces. If you are connected to the device with SSH, your connection may drop. You must reconnect using the console port.*

Data interface to use for management:

GigabitEthernet0/0

Specify a name for the interface [outside]:

outside-1

IP address (manual / dhcp) [dhcp]:

manual

IPv4/IPv6 address:

10.6.2.4

Netmask/IPv6 Prefix:

255.255.255.0

Default Gateway:

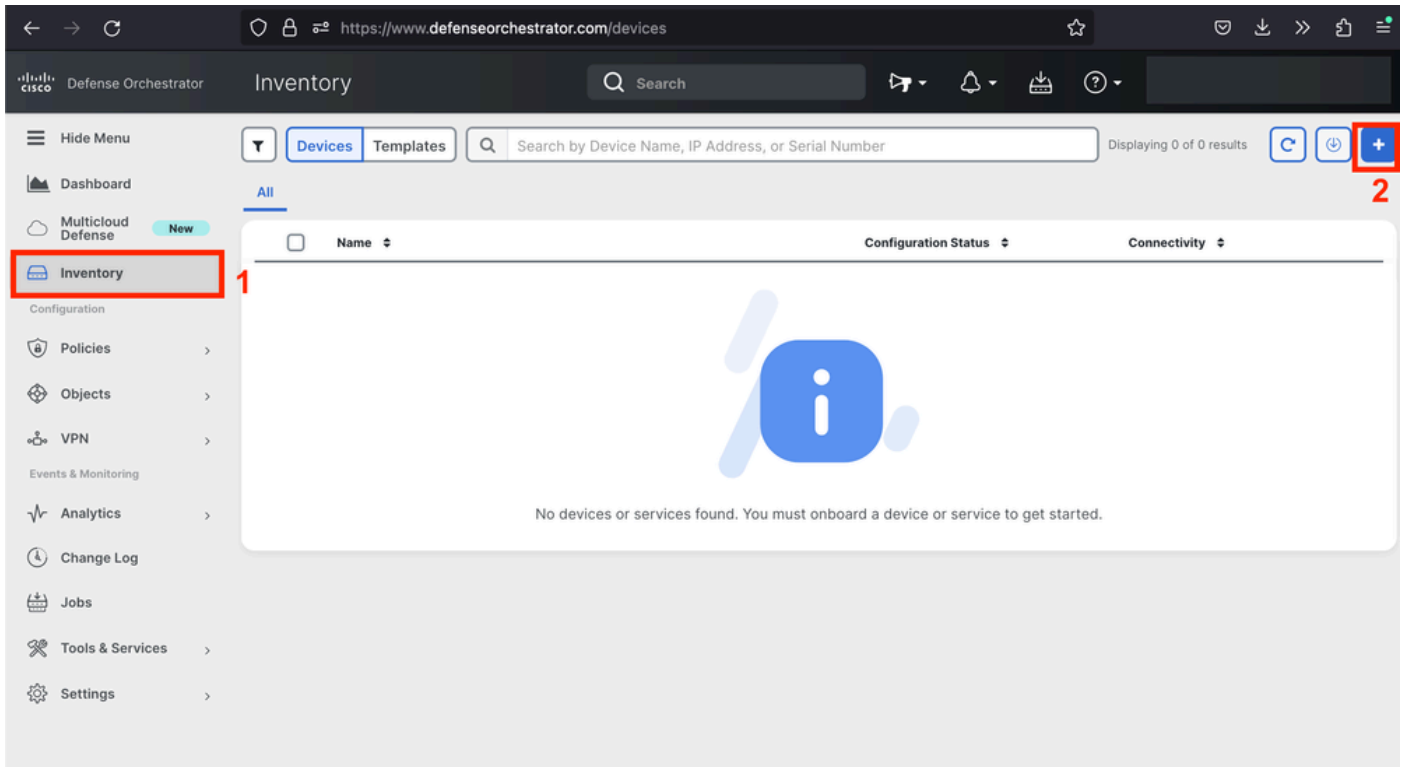
10.6.2.1

Tenere presente che l'interfaccia di gestione originale non può essere configurata per l'utilizzo di DHCP. Per verificare questa condizione, è possibile utilizzare il comando `show network`.

## FTD integrato con CDO

Questo processo incorpora l'FTD di Azure con CDO in modo che possa essere gestito da un FMC recapitato nel cloud. Il processo utilizza una chiave di registrazione CLI, che è utile se il dispositivo ha un indirizzo IP assegnato tramite DHCP. Altri metodi di caricamento, quali il provisioning log-touch e il numero di serie, sono supportati solo sulle piattaforme Firepower 1000, Firepower 2100 o Secure Firewall 3100.

Passaggio 1. Nel portale CDO passare a Inventario, quindi fare clic su Onboard option:



Pagina Magazzino

Passaggio 2. Fare clic nel riquadro FTD:

## Select a Device or Service Type

No Secure Device Connector found to communicate with some types of devices. [Set up a Secure Device Connector](#)



### ASA

Adaptive Security Appliance  
(8.4+)



### Multiple ASAs

Adaptive Security Appliance  
(8.4+)



### FTD

Cisco Secure  
Firewall Threat Defense

Meraki

### Meraki

Meraki Security Appliance



### Integrations

Enable basic CDO functionality for  
integrations



### AWS VPC

Amazon Virtual Private Cloud



### Duo Admin

Duo Admin Panel

Umbrella

### Umbrella Organization

View Umbrella Organization Policies  
from CDO



### Import

Import configuration for offline  
management

Introduzione all'FTD

Passaggio 3. Scegliere l'opzione Use CLI Registration key:



Firewall Threat Defense

**Important:** After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure policies from CDO after onboarding. [Learn more](#)



#### Use CLI Registration Key

Onboard a device using a registration  
key generated from CDO and applied  
on the device using the Command  
Line Interface.  
(FTD 7.0.3+ & 7.2+)



#### Use Serial Number

Use this method for low-touch  
provisioning or for onboarding  
configured devices using their serial  
number.  
(FTD 7.2+)



#### Deploy an FTD to a cloud environment

Deploy an FTD to a supported cloud  
environment; AWS, GCP and Azure

Uso della chiave di registrazione CLI

Passaggio 4. Copiare la chiave CLI iniziando dal comando configure manager:

1 Device Name **FTDv-Azure**

2 Policy Assignment **Access Control Policy: Default Access Control Policy**

3 Subscription License **Performance Tier: FTDv, License: Threat, Malware, URL License**

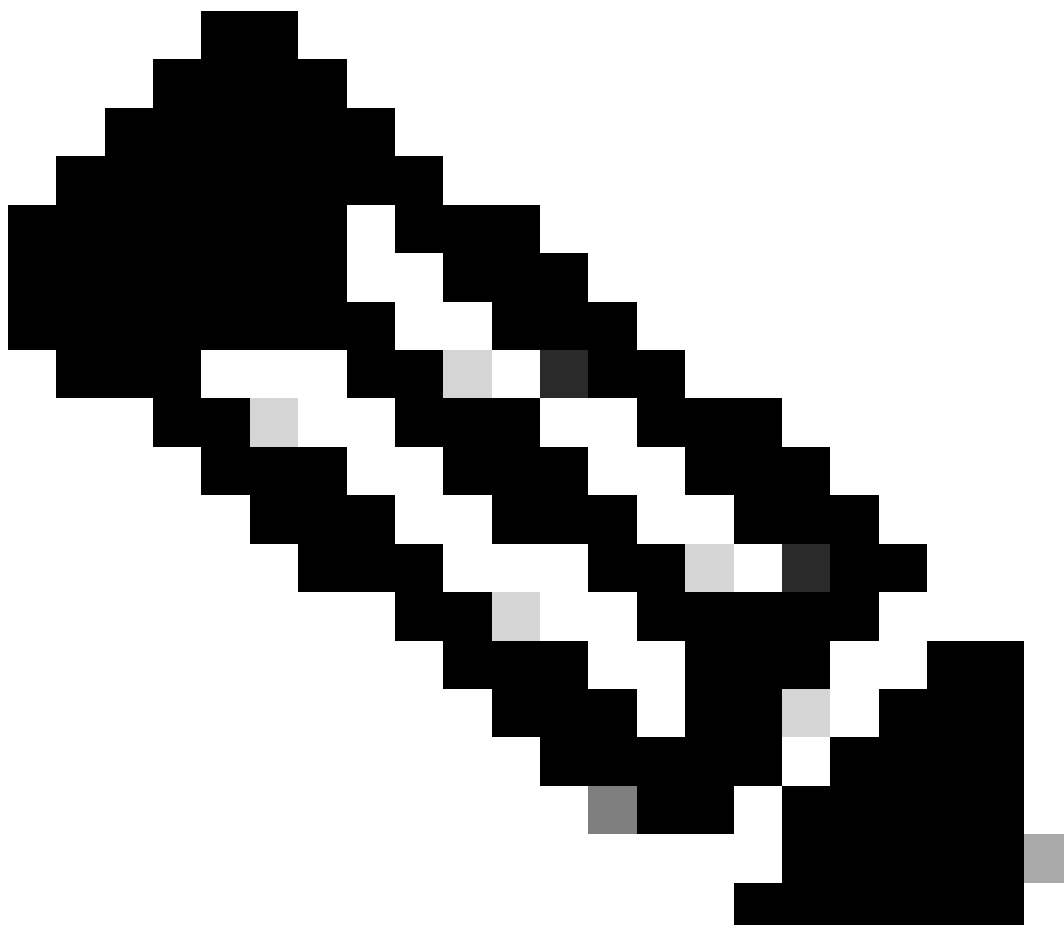
4 CLI Registration Key

- 1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)
- 2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com  
t67mPqC8cAW6GH2NhhhTUD4poWARdRr7 YJqFWzmpnfbJ6WANBeHTAhXnod9E7c1e cisco-cisco-  
systems--s1kaau.app.us.cdo.cisco.com
```

[Next](#)

Comando Copia Configura Gestione



Nota: la chiave CLI corrisponde al formato utilizzato nelle registrazioni di FTD con FMC

locali, dove è possibile configurare un NAT-ID per consentire la registrazione quando il dispositivo gestito è collegato a un dispositivo NAT: `configure manager add <fmc-hostname-or-ipv4> <registration-key> <nat-id> <display-name>`

Passaggio 5. Incollare il comando nella CLI FTD. Se la comunicazione ha esito positivo, è necessario ricevere questo messaggio:

```
Manager cisco-cisco-systems--s1kaau.app.us.cdo.cisco.com successfully configured.  
Please make note of reg_key as this will be required while adding Device in FMC.
```

Passaggio 6. Tornare al CDO e fare clic su Avanti:

3 Subscription License Performance Tier: FTDv, Licen

4 CLI Registration Key

- 1 Ensure the device's initial
- 2 Copy the CLI Key below and

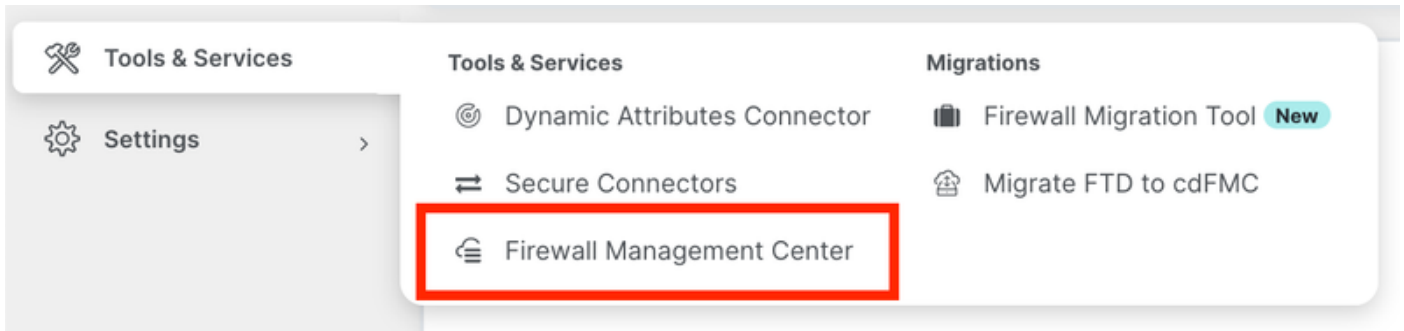
```
configure manager add  
t67mPqC8cAW6GH2NhhhTL  
systems--s1kaau.app.u
```

Next

Fare clic su Avanti.

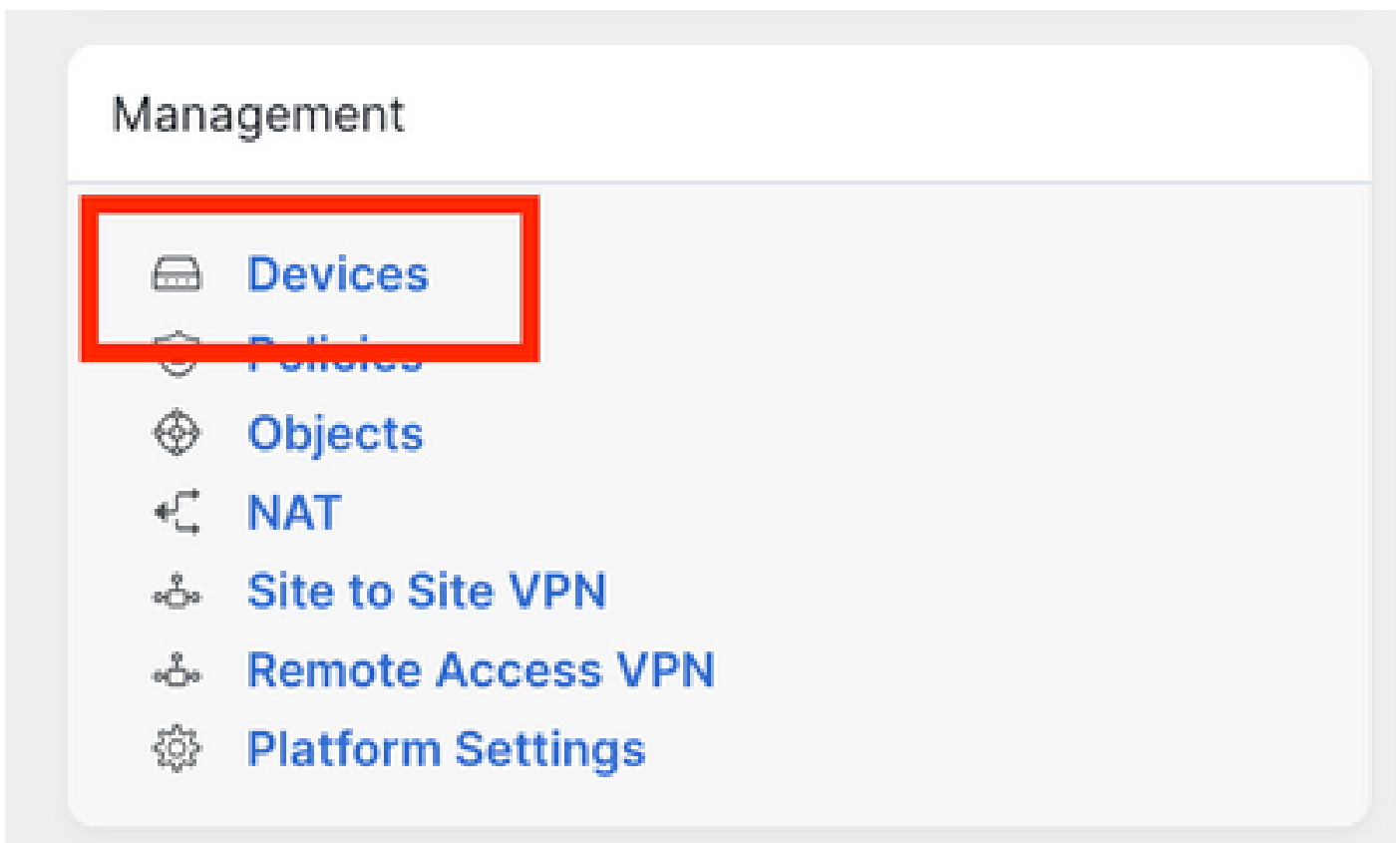
CDO continua il processo di registrazione e viene visualizzato un messaggio che indica che il completamento richiede molto tempo. È possibile controllare lo stato del processo di registrazione facendo clic sul collegamento Dispositivi nella pagina Servizi.

Passaggio 7. Accedere al CCP dalla pagina Strumenti e servizi.



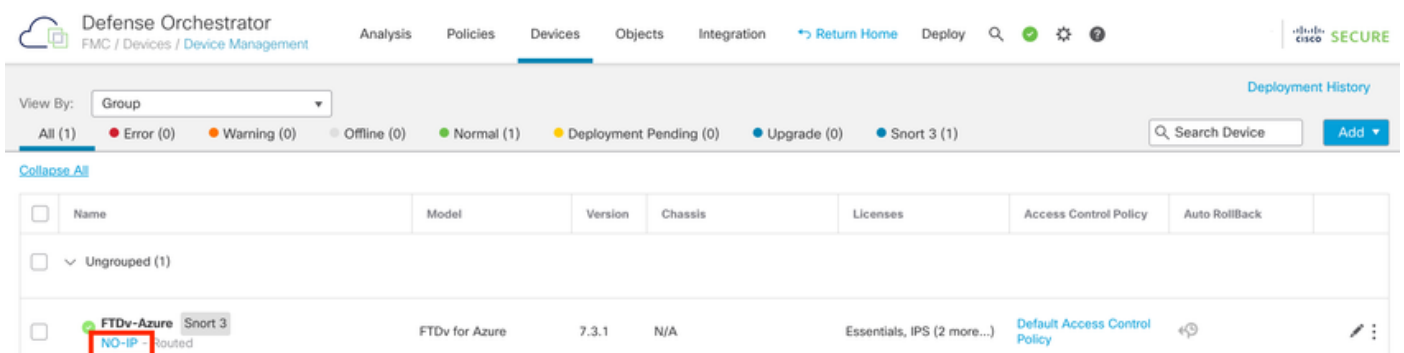
Accesso a cdFMC

Fare clic sul collegamento Dispositivi.



Fare clic su Dispositivi

Il FTD è ora integrato nel CDO e può essere gestito dal FMC distribuito nel cloud. Nell'immagine successiva è presente un NO-IP elencato sotto il nome del dispositivo. Ciò è previsto in un processo di caricamento che utilizza la chiave di registrazione CLI.







## Edit Physical Interface



General IPv4 IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

Name:  
outside-2

Enabled  
 Management Only

Description:

Mode:  
None

Security Zone:  
outside2-sz

Area di sicurezza per interfaccia dati ridondante

Passaggio 5. Si noti che ora entrambe le interfacce hanno il tag Manager Access. Verificare inoltre che l'interfaccia dati primaria sia stata assegnata a un'altra area di sicurezza:

FTDv-Azure Cisco Firepower Threat Defense for Azure Save Cancel

Device Routing Interfaces Inline Sets DHCP VTEP

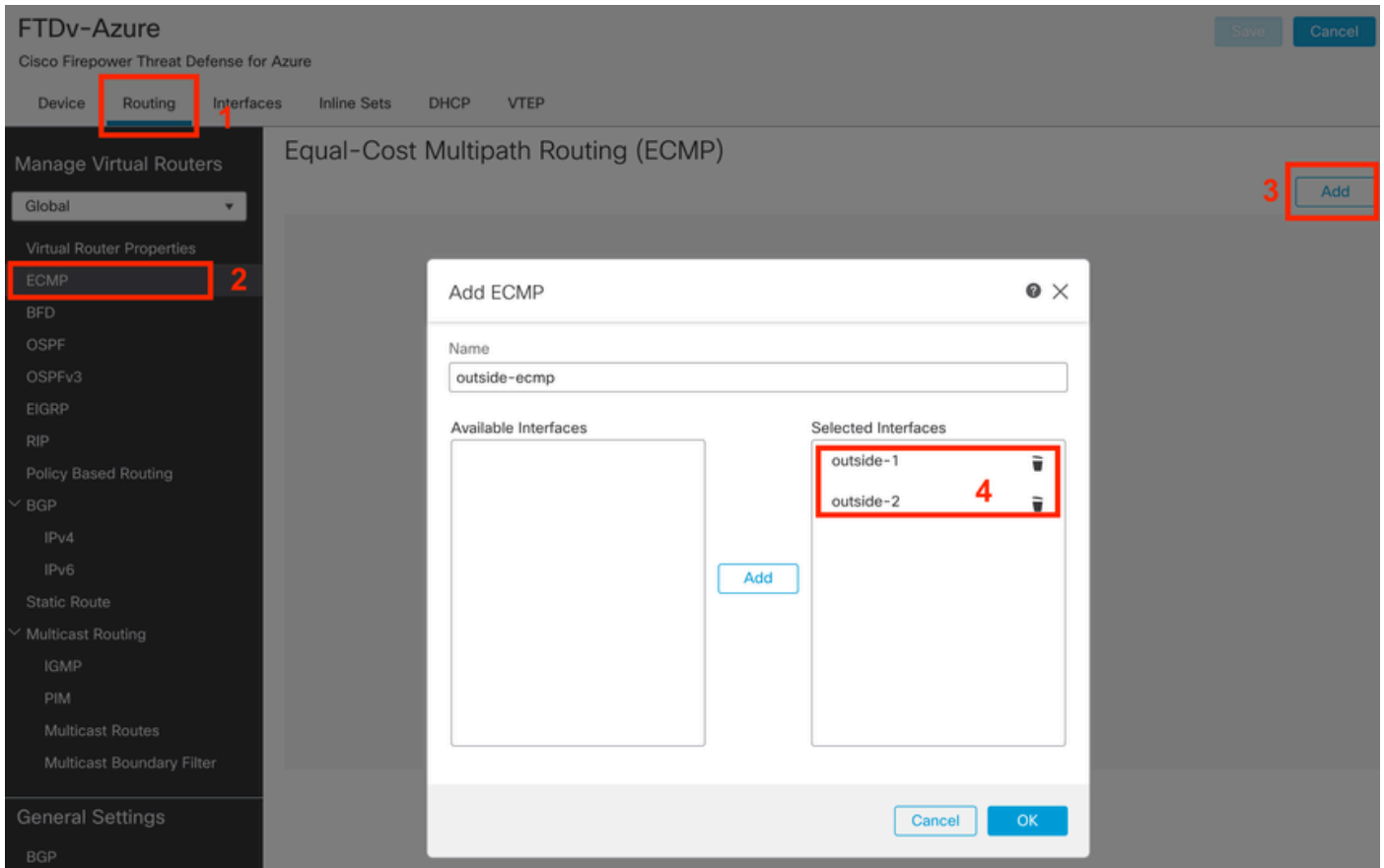
Search by name Sync Device Add Interfaces

Interface	Logical N...	Type	Security Z...	MAC Address (Active/Standby)	IP Address	Path...	Virtual Ro...
Diagnostic0/0	diagnostic	Phy				Disa...	Global
GigabitEthernet0/0 (Manager Access)	outside-1	Phy	outside1-sz		10.6.2.4/255.255.255.0(Static)	Disa...	Global
GigabitEthernet0/1 (Manager Access)	outside-2	Phy	outside2-sz		10.6.3.4/255.255.255.0(Static)	Disa...	Global

Revisione configurazione interfaccia

Nella sezione successiva, i passaggi da 6 a 10 hanno lo scopo di configurare due route predefinite di costo uguale per raggiungere il CDO, ognuna monitorata da un processo di rilevamento SLA indipendente. Il monitoraggio degli SLA garantisce l'esistenza di un percorso funzionale per comunicare con il CdFMC utilizzando l'interfaccia monitorata.

Passaggio 6. Passare alla scheda Instradamento e nel menu ECMP creare una nuova zona ECMP con entrambe le interfacce:

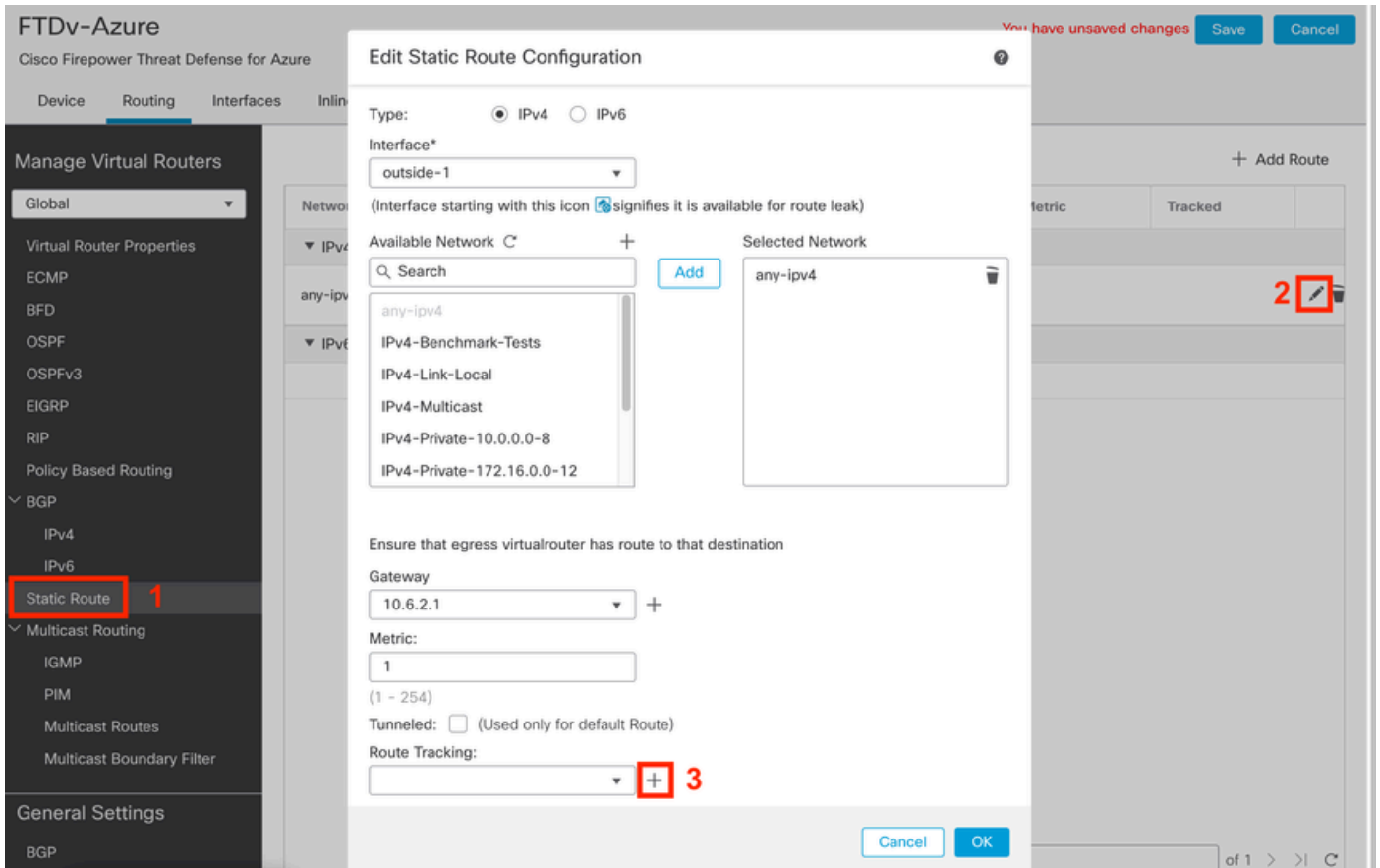


Configurare una zona ECMP

Fare clic su OK e su Salva.

Passaggio 7. Dalla scheda Instradamento, passare a Instradamenti statici.

Fare clic sull'icona a forma di matita per modificare il percorso principale. Quindi fare clic sul segno più per aggiungere un nuovo oggetto di rilevamento SLA:



Modifica route primaria per aggiungere il rilevamento SLA

Passaggio 8. Nell'immagine seguente sono evidenziati i parametri obbligatori per una registrazione funzionale dello SLA. Facoltativamente, è possibile regolare altre impostazioni come Numero di pacchetti, Timeout e Frequenza.

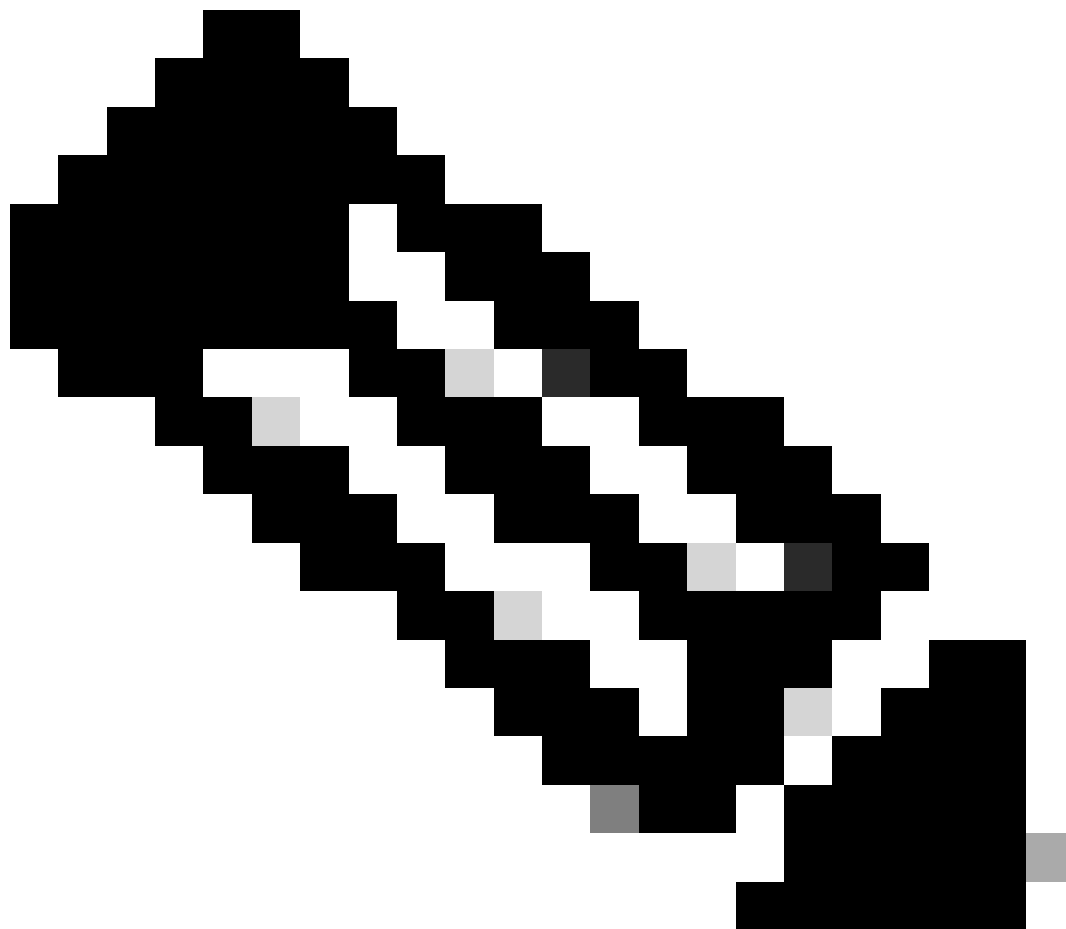
# Edit SLA Monitor Object



<b>Name:</b> <input type="text" value="outside1-sla"/>	<b>Description:</b> <input type="text"/>
<b>Frequency (seconds):</b> <input type="text" value="60"/> <small>(1-604800)</small>	<b>SLA Monitor ID*:</b> <input type="text" value="1"/>
<b>Threshold (milliseconds):</b> <input type="text" value="5000"/> <small>(0-60000)</small>	<b>Timeout (milliseconds):</b> <input type="text" value="5000"/> <small>(0-604800000)</small>
<b>Data Size (bytes):</b> <input type="text" value="28"/> <small>(0-16384)</small>	<b>ToS:</b> <input type="text" value="0"/>
<b>Number of Packets:</b> <input type="text" value="1"/>	<b>Monitor Address*:</b> <input type="text" value=""/>
<b>Available Zones</b>	<b>Selected Zones/Interfaces</b>
<input type="text" value="Search"/> outside1-sz outside2-sz	<input type="button" value="Add"/> <input type="text" value="outside1-sz"/>

In questo esempio Google DNS IP è stato usato per monitorare le funzionalità FTD per raggiungere Internet (e CDO) tramite l'interfaccia esterna 1. Fare clic su ok quando si è pronti.

---



Nota: assicurarsi di tenere traccia di un indirizzo IP che è già stato verificato come raggiungibile dall'interfaccia esterna FTD. Configurare una traccia con un indirizzo IP non raggiungibile può disattivare la route predefinita in questo FTD e impedirne la comunicazione con il CDO.

---

Passaggio 9. Fare clic su Salva e verificare che il nuovo rilevamento SLA sia assegnato al ciclo di lavorazione che punta all'interfaccia primaria:

## Route Tracking:



Tracciamento esterno di 1 contratto di servizio

Dopo aver fatto clic su OK, viene visualizzato un popup con il messaggio di AVVERTENZA successivo:

## Warning about Static Route

**This Static route is defined on the Defense Orchestrator Access Interface. Ensure the change is not affecting connectivity to the device**

OK

Avviso di configurazione

Passaggio 10. Fare clic su Add Route per aggiungere un nuovo instradamento per l'interfaccia dati ridondante. Nell'immagine successiva si noti che il valore della metrica per la route è lo stesso. Inoltre, la registrazione del contratto di servizio ha un ID diverso:

# Add Static Route Configuration



Type:  IPv4  IPv6

Interface\*

outside-2

(Interface starting with this icon signifies it is available for route leak)

Available Network



Search

Add

any-ipv4

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Selected Network

any-ipv4

Gateway\*

10.6.3.1



Metric:

1

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

outside2-sla



Cancel

OK

Configura route statica ridondante



# Edit SLA Monitor Object



Name:

outside2-sla

Description:

Frequency (seconds):

60

(1-604800)

SLA Monitor ID\*:

2

Threshold (milliseconds):

5000

(0-60000)

Timeout (milliseconds):

5000

(0-604800000)

Data Size (bytes):

28

(0-16384)

ToS:

0

Number of Packets:

1

Monitor Address\*

Available Zones

Search

outside1-sz

outside2-sz

Add

Selected Zones/Interfaces

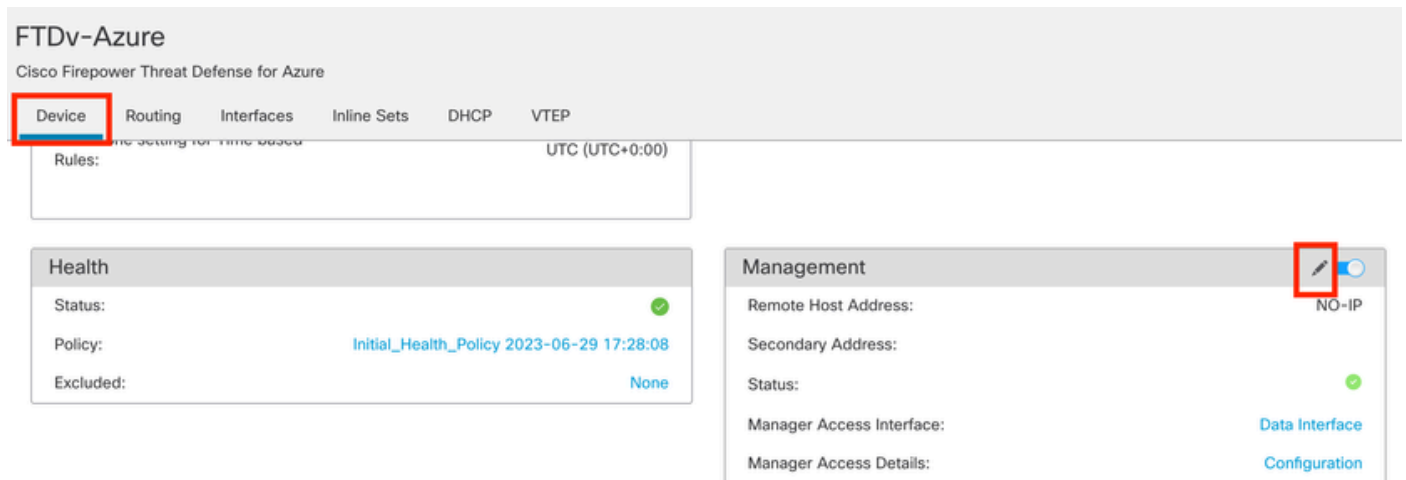
outside2-sz

Cancel

Save

Fare clic su Save (Salva).

Passaggio 11. Facoltativamente, è possibile specificare l'indirizzo IP dell'interfaccia dati secondaria in Dispositivo > Gestione. Anche se, questo non è richiesto, dato che il metodo di caricamento attuale ha utilizzato il processo di registrazione della chiave CLI:



(Facoltativo) Specificare un indirizzo IP per l'interfaccia dati ridondante nel campo Gestione

Passaggio 12. Distribuire le modifiche.

(Facoltativo) Impostare un costo di interfaccia per una modalità interfaccia attiva/di backup:

Per impostazione predefinita, la gestione ridondante tramite interfaccia dati utilizza il metodo Round Robin per distribuire il traffico di gestione tra entrambe le interfacce. In alternativa, se un collegamento WAN ha una larghezza di banda maggiore dell'altro e si preferisce che sia il collegamento di gestione principale mentre l'altro rimane come backup, è possibile assegnare al collegamento principale un costo pari a 1 e al collegamento di backup un costo pari a 2. Nell'esempio successivo, l'interfaccia Gigabit Ethernet0/0 viene mantenuta come collegamento WAN principale, mentre Gigabit Ethernet0/1 funge da collegamento per la gestione dei backup:

1. Passare a Dispositivi > FlexConfig link e creare un criterio flexConfig. Se esiste già un criterio flexConfig configurato e assegnato al FTD, modificarlo:

Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
<b>FlexConfig</b>	Site to Site Monitoring	
Certificates		

Accesso al menu FlexConfig

## 2. Creare un nuovo oggetto FlexConfig:

- Assegnare un nome all'oggetto FlexConfig.
- Scegliere Everytime e Append nelle sezioni Deployment e Type rispettivamente.
- Impostare il costo delle interfacce con i comandi successivi, come illustrato nell'immagine 22.
- Fare clic su Save (Salva).

```
<#root>
```

```
interface GigabitEthernet0/0
```

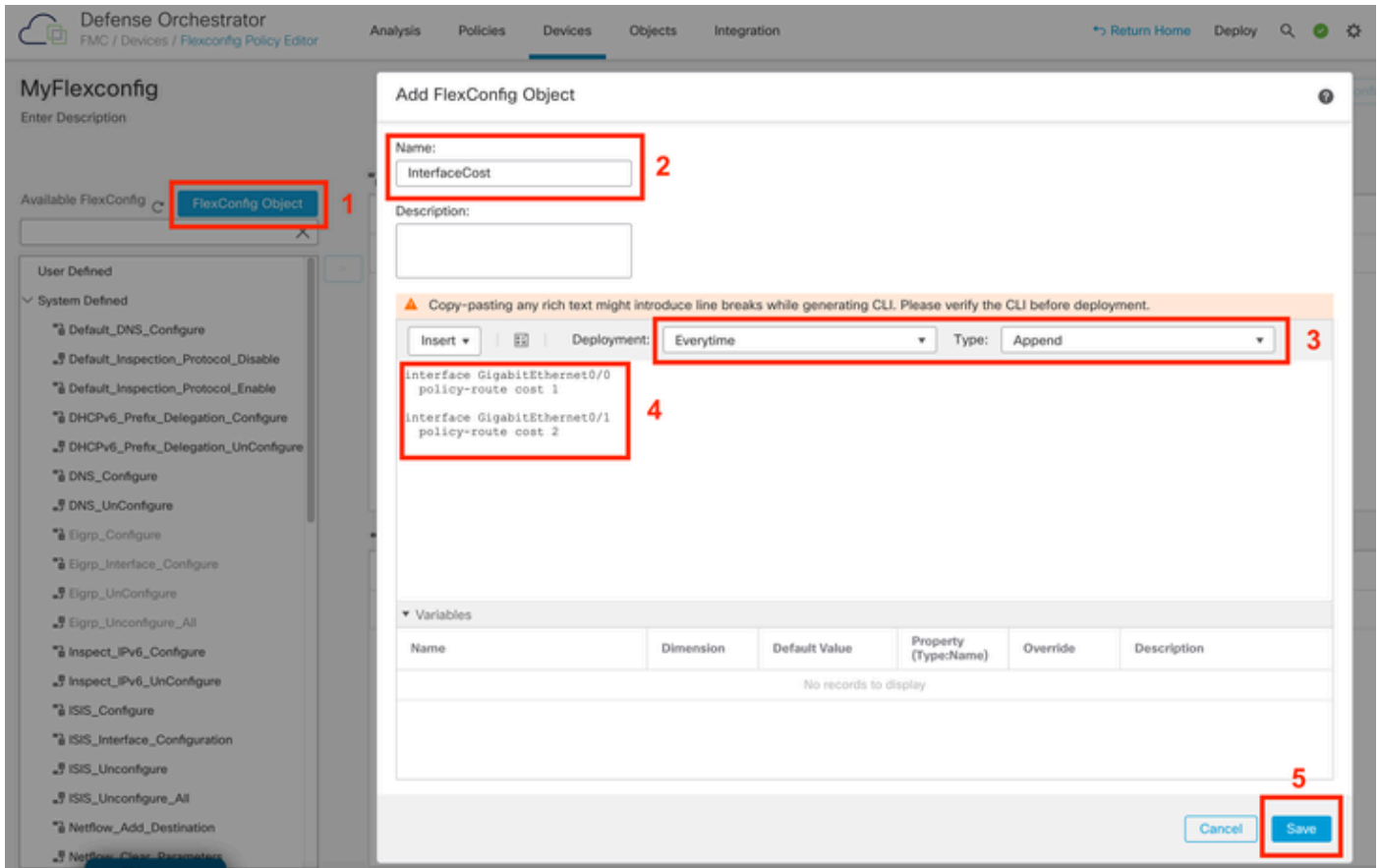
```
  policy-route cost 1
```

<=== A cost of 1 means this will be the primary interface for management communication with CDO tenant.

```
interface GigabitEthernet0/1
```

```
  policy-route cost 2
```

<=== Cost 2 sets this interface as a backup interface.



Aggiunta di un oggetto Flexconfig

3. Scegliere l'oggetto creato di recente e aggiungerlo alla sezione Append FlexConfigs selezionata come illustrato nella figura. Salvare le modifiche e distribuire la configurazione.

Defense Orchestrator Flexconfig Policy Editor

Analysis Policies Devices Objects Integration [Return Home](#) **Deploy** 5

MyFlexconfig Migrate Config Preview Config **Save** 4 Cancel Policy Assignments (1)

Enter Description

Available FlexConfig FlexConfig Object

- ✓ User Defined
  - InterfaceCost** 1
- System Defined
  - Default\_DNS\_Configure
  - Default\_Inspection\_Protocol\_Disable
  - Default\_Inspection\_Protocol\_Enable
  - DHCPv6\_Prefix\_Delegation\_Configure
  - DHCPv6\_Prefix\_Delegation\_UnConfigure
  - DNS\_Configure
  - DNS\_UnConfigure
  - Eigrp\_Configure
  - Eigrp\_Interface\_Configure
  - Eigrp\_UnConfigure
  - Eigrp\_Unconfigure\_All
  - Inspect\_IPv6\_Configure
  - Inspect\_IPv6\_UnConfigure
  - ISIS\_Configure
  - ISIS\_Interface\_Configuration
  - ISIS\_Unconfigure
  - ISIS\_Unconfigure\_All
  - Netflow\_Add\_Destination

Selected Prepend FlexConfigs

#	Name	Description

Selected Append FlexConfigs

#	Name	Description
1	InterfaceCost	

Assegnazione dell'oggetto al criterio Flexconfig

#### 4. Distribuire le modifiche.

## Verifica

1. Per procedere alla verifica, usare il comando show network. Viene creata una nuova istanza per l'interfaccia di gestione ridondante:

```
> show network
```

```
<<----- output omitted for brevity ----->>
```

```
=====[ eth0 ]=====
State : Enabled
Link : Up
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 60:45:BD:D8:62:D7
-----[ IPv4 ]-----
Configuration : Manual
```

```
Address : 10.6.0.4
Netmask : 255.255.255.0
-----[ IPv6 ]-----
Configuration : Disabled
```

```
=====[ Proxy Information ]=====
State : Disabled
Authentication : Disabled
. . .
```

```
=====[ GigabitEthernet0/0 ]=====
State : Enabled
Link : Up
Name : outside-1
MTU : 1500
MAC Address : 60:45:BD:D8:6F:5C
-----[ IPv4 ]-----
Configuration : Manual
Address : 10.6.2.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
-----[ IPv6 ]-----
Configuration : Disabled
```

```
=====[ GigabitEthernet0/1 ]=====
State : Enabled
Link : Up
Name : outside-2
MTU : 1500
MAC Address : 60:45:BD:D8:67:CA
-----[ IPv4 ]-----
Configuration : Manual
Address : 10.6.3.4
Netmask : 255.255.255.0
Gateway : 10.6.3.1
-----[ IPv6 ]-----
Configuration : Disabled
```

2. L'interfaccia fa ora parte del dominio sftunnel. È possibile confermare questa condizione con le interfacce show tunnel e i comandi show running-config tunnel:

```
<#root>
```

```
>
```

```
show sftunnel interfaces
```

```
Physical Interface Name of the Interface
GigabitEthernet0/0 outside-1
GigabitEthernet0/1 outside-2
```

```
>
```

```
show running-config sftunnel
```

```
sftunnel interface outside-2
sftunnel interface outside-1
```

```
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

3. Viene automaticamente specificata una route basata su criteri. Se non è stato specificato un costo di interfaccia, l'opzione adaptive-interface imposta l'elaborazione round robin in modo da bilanciare il carico del traffico di gestione tra entrambe le interfacce:

```
<#root>
```

```
>
```

```
show running-config route-map
```

```
!
route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346 permit 5
 match ip address FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
 set adaptive-interface cost outside-1 outside-2
```

```
>
```

```
show access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392
```

```
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392; 1 elements; name hash: 0x8e8cb508
access-list FMC_GEN_056473829_RBD_DUAL_WAN_ACL_165748392 line 1 extended permit tcp any any eq 8305 (hi
```

4. Utilizzare il comando show running-config interface <interface> per controllare le impostazioni dell'interfaccia:

```
<#root>
```

```
>
```

```
show running-config interface GigabitEthernet 0/0
```

```
!
interface GigabitEthernet0/0
 nameif outside-1
 security-level 0
 zone-member outside-ecmp
 ip address 10.6.2.4 255.255.255.0
 policy-route cost 1
```

```
>
```

```
show running-config interface GigabitEthernet 0/1
```

```
!
interface GigabitEthernet0/1
 nameif outside-2
 security-level 0
 zone-member outside-ecmp
 ip address 10.6.3.4 255.255.255.0
```

```
policy-route cost 2
```

Per controllare il rilevamento delle route configurate è possibile utilizzare alcuni comandi aggiuntivi:

```
<#root>
```

```
>
```

```
show track
```

```
Track 1
```

```
Response Time Reporter 2 reachability
```

```
Reachability is Up
```

```
<===== Ensure reachability is up for the monitored interf
```

```
2 changes, last change 09:45:00
```

```
Latest operation return code: OK
```

```
Latest RTT (milliseconds) 10
```

```
Tracked by:
```

```
STATIC-IP-ROUTING 0
```

```
Track 2
```

```
Response Time Reporter 1 reachability
```

```
Reachability is Up
```

```
<===== Ensure reachability is up for the monitored interf
```

```
2 changes, last change 09:45:00
```

```
Latest operation return code: OK
```

```
Latest RTT (milliseconds) 1
```

```
Tracked by:
```

```
STATIC-IP-ROUTING 0
```

```
>
```

```
show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route, + - replicated route
```

```
SI - Static InterVRF, BI - BGP InterVRF
```

```
Gateway of last resort is 10.6.3.1 to network 0.0.0.0
```

```
S* 0.0.0.0 0.0.0.0 [1/0] via 10.6.3.1, outside-2
```

```
[1/0] via 10.6.2.1, outside-1
```

```
C 10.6.2.0 255.255.255.0 is directly connected, outside-1
```

```
L 10.6.2.4 255.255.255.255 is directly connected, outside-1
```

```
C 10.6.3.0 255.255.255.0 is directly connected, outside-2
```

```
L 10.6.3.4 255.255.255.255 is directly connected, outside-2
```

## Informazioni correlate



- [Supporto tecnico Cisco e download](#)
- [Gestione della difesa dalle minacce dei firewall con il centro di gestione dei firewall distribuito tramite cloud in Cisco Defense Orchestrator](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).